INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA Y CIENCIAS SOCIALES Y ADMINISTRATIVAS

LICENCIATURA EN INGENIERÍA EN INFORMÁTICA

"Web API Security Scanner"

PRESENTAN

- **Gonzalez Calzada Maximiliano**
- **Hernandez Garcia Juan Jose**
- **Maldonado Martínez Kevin Noel**
- **Martínez Lagunas Andrik Jeovany**
- **Muñoz Castro Angel Daniel**

DOCENTE

Ortega Avalos Julia Alicia

ASIGNATURA

Seguridad Informática

SECUENCIA

4NM42

25 de noviembre de 2024

1. Objetivo

Desarrollar una herramienta que escanee las API web en busca de vulnerabilidades de seguridad, asegurando que sean sólidas contra amenazas comunes y proporcionando recomendaciones de mejora. Puede ayudar a demostrar el cumplimiento de es- tas normativas. La herramienta no solo identificará vulnerabilidades ya existentes, sino que también puede servir como un medio proactivo para detectar configuraciones inseguras y prácticas deficientes en la implementación de APIs.

2. Alcance

2.1. Cobertura de Seguridad:

- **Autenticación y Autorización**: Revisar las configuraciones de autenticación (JWT, OAuth) y control de acceso.
- **Validación de Entrada**: Identificar vulnerabilidades de inyección (SQL, XSS, comandos).
- **Limitación de Tarifas y Exposición de Datos Sensibles**: Comprobar la limitación de tasa para evitar abusos y verificar si se transmiten datos sensibles sin cifrado.
- **Detección de Amenazas Comunes**: Enfocarse en las vulnerabilidades descritas en el OWASP API Security Top Ten.

2.2. Límites del Proyecto:

- **Exclusiones**: La herramienta no se enfocará en realizar pruebas de rendimiento o funcionalidad de la API; su único enfoque será la seguridad.
- **Limitaciones Técnicas**: El alcance inicial del proyecto no incluirá integración avanzada con sistemas de terceros para generación de reportes o monitoreo, aunque esta funcionalidad podría considerarse en versiones futuras.

3. Justificación

En México, el panorama de ciberseguridad ha mostrado un aumento significativo en los incidentes relacionados con APIs web. Casos recientes han expuesto vulnerabilidades críticas, como el hackeo a sistemas gubernamentales que resultó en la filtración de datos sensibles en 2022, y los ataques al sector financiero reportados por la Comisión Nacional Bancaria y de Valores (CNBV) en 2023, donde APIs bancarias fueron explotadas para realizar fraudes y acceder a información confidencial. Estos incidentes resaltan la urgente necesidad de fortalecer la seguridad en APIs, especialmente en un contexto donde los cibercriminales emplean tácticas cada vez más sofisticadas para identificar y aprovechar puntos débiles.

En la actualidad, las API son fundamentales para el funcionamiento de aplicaciones modernas, permitiendo la comunicación entre diferentes sistemas y servicios. Con el aumento de su uso, también ha crecido la superficie de ataque, haciendo que la seguridad de las API sea una prioridad. A continuación se detallan las razones que apoyan la necesidad de un escáner de seguridad para APIs web:

- **Creciente Dependencia de APIs**: Con la propagación de arquitecturas basadas en microservicios y el uso extensivo de servicios web, las APIs se han convertido en un punto de entrada crucial para las aplicaciones. Esto las convierte en un objetivo atractivo para los atacantes.

- **Vulnerabilidades Comunes**: Existen vulnerabilidades comunes en las APIs, como las descritas en el OWASP API Security Top Ten. Un escáner automatizado puede ayudar a identificar y mitigar estas vulnerabilidades antes de que sean explotadas.
- **Automatización y Eficiencia**: Realizar análisis de seguridad manualmente es intensivo en tiempo y recursos. Una herramienta automatizada permite escanear múltiples APIs de forma eficiente, liberando a los equipos de seguridad para que se concentren en análisis más profundos y en la remediación de problemas detectados.
- **Mejora Continua en la Seguridad**: La generación de informes detallados con recomendaciones proporciona a los desarrolladores y equipos de seguridad una guía para mejorar continuamente la postura de seguridad de sus APIs.
- **Educación y Conciencia**: Incluir una interfaz amigable y documentación clara no solo hace que la herramienta sea accesible, sino que también educa a los usuarios sobre las prácticas de seguridad y la importancia de proteger sus APIs.
- **Cumplimiento Normativo**: Muchas organizaciones están sujetas a regulaciones que exigen la implementación de prácticas de seguridad adecuadas. Un escáner de seguridad puede ayudar a demostrar el cumplimiento de estas normativas.
- **Proactividad ante Amenazas**: La herramienta no solo identificará vulnerabilidades ya existentes, sino que también puede servir como un medio proactivo para detectar configuraciones inseguras y prácticas deficientes en la implementación de APIs. Adoptar un enfoque proactivo en la seguridad permite que las empresas se anticipen a posibles ataques y mantengan su infraestructura más segura.

4. Marco teórico

4.1. Definición de Seguridad

La seguridad se refiere al conjunto de medidas, procesos y prácticas diseñadas para proteger recursos valiosos frente a posibles riesgos, amenazas o accesos no autorizados. En un sentido amplio, abarca la protección de bienes tangibles e intangibles, asegurando su disponibilidad, integridad y confidencialidad.

4.2. Seguridad Informática

La seguridad informática se centra en la protección de sistemas de información, redes y datos frente a amenazas que puedan comprometer su confidencialidad, integridad o disponibilidad. Esto incluye la implementación de controles técnicos, como cifrado y firewalls, y procesos administrativos para prevenir accesos no autorizados y minimizar el impacto de posibles ataques. La seguridad informática es crucial en un mundo donde los datos digitales son un recurso estratégico tanto para individuos como para organizaciones.

4.3. Seguridad en la Red

La seguridad en la red engloba las políticas, tecnologías y prácticas utilizadas para proteger la infraestructura de redes y los datos que se transfieren a través de ellas. Esto incluye prevenir ataques como interceptación de datos (sniffing), denegación de servicio (DoS), intrusiones y malware. Las medidas comunes en la seguridad de red incluyen el uso de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y protocolos de cifrado como TLS/SSL.

4.4. Seguridad en la Nube

La seguridad en la nube es el conjunto de políticas, tecnologías y controles diseñados para proteger datos, aplicaciones y servicios alojados en plataformas de computación en la nube. Incluye aspectos como la protección de datos en reposo y en tránsito, el cumplimiento de normativas, y la gestión de accesos y permisos en entornos compartidos. La adopción masiva de servicios en la nube ha aumentado los riesgos, haciendo esencial la implementación de medidas robustas como el cifrado, autenticación multifactor y auditorías regulares.

4.5. Introducción a las APIs Web

4.5.1. Definición

Las APIs (Interfaz de Programación de Aplicaciones) permiten que diferentes aplicaciones se comuniquen entre sí. Son cruciales en la arquitectura de software moderna, especialmente en aplicaciones web y móviles. Son mecanismos que permiten que diferentes aplicaciones y sistemas intercambien datos y funciones entre sí. Son esenciales en el entorno digital actual, especialmente en aplicaciones web y móviles, donde facilitan la interoperabilidad y la integración de diversas funcionalidades. Las APIs son la columna vertebral de arquitecturas modernas como los microservicios, permitiendo que distintos componentes de software se comuniquen y trabajen juntos sin estar directamente acoplados.

4.5.2. Importancia

Facilitan la integración y la interoperabilidad, pero también presentan riesgos de seguridad que deben ser gestionados adecuadamente. La popularidad de las APIs ha crecido junto con el uso de servicios en la nube, lo que ha incrementado su papel en las estrategias de negocio de las organizaciones. Sin embargo, esta integración trae consigo importantes riesgos de seguridad, ya que las APIs se exponen frecuentemente a redes públicas, convirtiéndolas en un blanco atractivo para atacantes. Una API sin las medidas de seguridad adecuadas puede ser la puerta de entrada para amenazas que afecten la integridad, confidencialidad y disponibilidad de los sistemas empresariales. La seguridad en las APIs implica implementar mecanismos de autenticación, autorización, validación de datos y monitoreo constante para mitigar estos riesgos.

4.6. La Seguridad Informática Relacionados con las APIs

En el contexto de seguridad informática, existen varios subtemas clave que se aplican específicamente a la seguridad de APIs:

- **Autenticación y Autorización**: La autenticación asegura que solo usuarios válidos accedan a una API, mientras que la autorización define los permisos y el nivel de acceso que cada usuario posee. Los estándares como OAuth 2.0 y JWT (JSON Web Tokens) son ampliamente utilizados en la autenticación de APIs para proporcionar acceso controlado y seguro.
- **Integridad de Datos**: Este principio garantiza que la información transmitida a través de la API no sea alterada durante el tránsito. La integridad de datos puede asegurarse mediante el uso de protocolos como HTTPS y el cifrado de datos sensibles, evitando ataques que alteren la información durante su transmisión.
- **Monitoreo y Registro**: Es fundamental registrar y monitorear las actividades dentro de una API para detectar comportamientos anómalos que puedan ser indicativos de intentos de ataque. Herramientas como los sistemas de detección de intrusiones (IDS) pueden integrarse para alertar sobre accesos inusuales o patrones de solicitudes sospechosas.

4.7. Amenazas Comunes a las APIs

- **Inyección SQL**: Permite a los atacantes ejecutar consultas maliciosas en la base de datos.
- **XSS**: Aprovecha la confianza del navegador en las API para ejecutar código en el contexto de un usuario.
- **Falsificación de solicitudes entre sitios (CSRF)**: Permite a un atacante hacer solicitudes en nombre de un usuario autenticado.
- **Desbordamiento de datos**: Implica enviar un volumen alto de datos a la API con el objetivo de desestabilizar o hacerla inaccesible.

4.8. OWASP y la Seguridad en APIs

El Open Web Application Security Project (OWASP) ha publicado una lista de los diez riesgos principales para la seguridad de APIs, conocida como OWASP API Security Top Ten. Este listado destaca vulnerabilidades comunes como la autenticación rota, la exposición excesiva de datos y la falta de limitación de tasas. La guía OWASP es una referencia fundamental en el desarrollo seguro de APIs, ya que proporciona recomendaciones prácticas para abordar las amenazas de seguridad más relevantes en entornos de API.

4.9. La Seguridad en APIs en el Contexto Empresarial

Las empresas de sectores como finanzas, salud y comercio electrónico dependen cada vez más de las APIs para optimizar operaciones, gestionar datos y facilitar la integración con terceros. Sin embargo, según un informe de Akamai, el 78 % de las organizaciones han experimentado incidentes de seguridad relacionados con APIs en el último año. Además, las vulnerabilidades en APIs pueden ocasionar pérdidas anuales de hasta 87 mil millones de dólares, según Businesswire. Por lo tanto, asegurar estas interfaces se convierte en una prioridad no solo para proteger los activos digitales y la información confidencial, sino también para cumplir con normativas y regulaciones de seguridad.

4.10. Estrategias de seguridad para las APIs

Implementar estrategias de seguridad en APIs implica un enfoque multidimensional que incluye las siguientes prácticas:

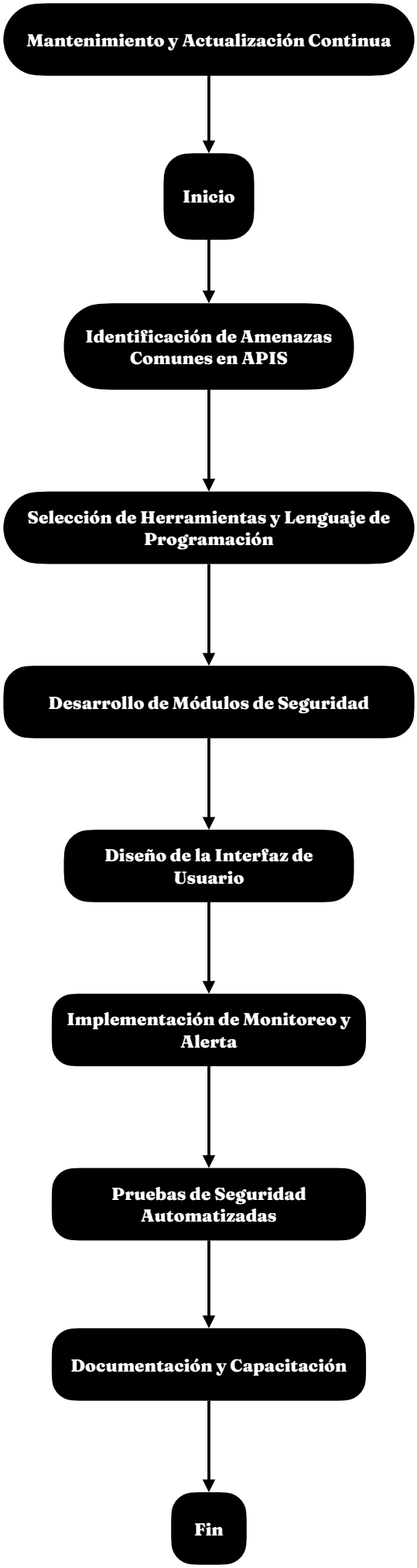
- **Autenticación y Autorización Fortalecidas**: Usar autenticación multifactor y revisar permisos con regularidad.
- **Limitación de Tasas (Rate Limiting)**: Restringir el número de solicitudes permitidas en un tiempo determinado para evitar ataques de denegación de servicio (DoS).
- **Validación de Datos y Filtrado de Entradas**: Validar los datos que ingresan a la API para evitar inyecciones maliciosas.
- **Cifrado de Comunicación**: Usar HTTPS para garantizar que los datos en tránsito estén protegidos contra interceptaciones.

5. Planteamiento de la solución

- **Identificación de Amenazas Comunes en APIs**: Revise el OWASP API Security Top Ten y otras normativas de seguridad para reconocer las vulnerabilidades más frecuentes en APIs.

- **Selección de Herramientas y Lenguaje de Programación**: Escoja un lenguaje adecuado (por ejemplo, Python o JavaScript) y herramientas de escaneo de seguridad (como OWASP ZAP o Burp Suite) que se integren efectivamente para identificar y mitigar riesgos.
- **Desarrollo de Módulos de Seguridad**: Implemente módulos específicos para detectar vulnerabilidades, como autenticación, autorización, inyección de SQL, XSS, y otros. Cada módulo debe ser capaz de realizar pruebas automatizadas y reportar sus hallazgos.
- **Diseño de la Interfaz de Usuario**: Cree una interfaz intuitiva, ya sea web o en línea de comandos, que permita a los usuarios configurar las API a escanear, seleccionar parámetros y monitorear el progreso de los escaneos.
- **Implementación de Monitoreo y Alerta**: Configure un sistema de monitoreo y alertas en tiempo real para detectar actividad sospechosa y registrar logs detallados de cada interacción de la API.
- **Pruebas de Seguridad Automatizadas**: Realice pruebas automatizadas y pruebas de penetración en entornos controlados, usando datos simulados para verificar la capacidad de detección y respuesta ante ataques.
- **Documentación y Capacitación**: Desarrolle documentación clara y detallada sobre cómo usar la herramienta, interpretando resultados y aplicando recomendaciones de seguridad. Incluya guías prácticas para el equipo de desarrollo y personal de seguridad.
- **Mantenimiento y Actualización Continua**: Programe revisiones y actualizaciones regulares de la herramienta para garantizar que se mantenga al día con nuevas vulnerabilidades y mejoras de seguridad en APIs.

6. Diagrama de procesos


Mantenimiento y Actualización Continua
Inicio
Identificación de Amenazas Comunes en APIS
Selección de Herramientas y Lenguaje de Programación
Desarrollo de Módulos de Seguridad
Diseño de la Interfaz de Usuario
Implementación de Monitoreo y Alerta
Pruebas de Seguridad Automatizadas
Documentación y Capacitación
Fin

7. Planeación

	Equipo 2: Seguridad informática 4NM42						Octubre			
ID	Actividad	Fecha de Inicio	Fecha de Fin	Duración (Días)	Dependecias	Responsable	Semana 1	Semana 2	Semana 3	Semana 4
	PROYECTO "Web API Security Scanner" - Seguridad Informática									
1	**PROPUESTA DE PROYECTO**									
2	Lluvia de ideas de posibles proyectos a realizar									
3	Elección de proyecto				2					
4	Definición de idea de proyecto				3					
5	**DOCUMENTACION DEL PROYECTO**									
6	Creacion del archivo colaborativo en Word para la documentación									
7	Crear el archivo de planeacion del proyecto en Excel									
8	Definir el rode map para el desarrollo del proyecto en el archivo de Excel				7					
9	Definir el nombre de proyecto				1					
10	**Objetivo del proyecto**									
11	Desarrollo del objetivo principal del proyecto				1					
12	Definir las caracteristicas clave dentro del objetivo del proyecto				11					
13	Definir los pasos para la implementación dentro del objetivo				11					
14	**Alcance del proyecto**									
15	Definicion del alcance sobre cobertura del proyecto				1					
16	Definicion del alcance sobre los limites del proyecto				1					
17	**Justificación del proyecto**									
18	Desarrollo de la justificación del proyecto				1					
19	**Marco teórico del proyecto**									
20	Definicion del marco teorico: Introduccion a las APIs Web				1					
21	Definicion del marco teorico: Amenazas comunes a las APIs				1					
22	**1ra Revision de proyecto**									
23	Retroalimentacion en la documentación del proyecto				1,5,10,14,17,19					
24	Corrección de errores y orden de la documentación				23					
25	**Planteamiento de la solución**									
26	Definir el planteamiento de la solucion del proyecto				1,5,10,14,17,19					
27	Definir el proceso a realizar para llevar a cabo la solucion del proyecto				26					
28	Crear el diagrama de flujo del proceso de solucion del proyecto				27					
29	Realizar el diagrama de casos de uso del proyecto				26					
30	**PROTOTIPO**									
31										
32	**DEMO**									
33										
34	**CONCLUSIONES**									
35										
36	**BIBLIOGRAFÍA**									
37										
38	**PRESENTACIÓN EN POWERPOINT**									
39										
40	**ARREGLAR DOCUMENTACIÓN**									
41										
42	**ENSAYO O PRESENTACIÓN**									
43										
44	**ENTREGA DE DOCUMENTACIÓN**									
45	**RELACION COLOR-INTEGRANTE**									
	Hernandez Garcia Juan Jose									
	Martínez Lagunas Andrik Jeovany									
	Muñoz Castro Angel Daniel									
	Maldonado Martínez Kevin Noel									
	Gonzalez Calzada Maximiliano									